

<p>David H. Krieger, Esq. Nevada Bar No. 9086 George Haines, Esq. Nevada Bar No. 9411 HAINES &amp; KRIEGER, LLC 8985 S. Eastern Ave., Suite 350 Henderson, NV 89123 Phone: (702) 880-5554 FAX: (702) 385-5518 dkrieger@hainesandkrieger.com</p> <p>Matthew I. Knepper, Esq. Nevada Bar No. 12796 Miles N. Clark, Esq. Nevada Bar No. 13848 KNEPPER &amp; CLARK LLC 10040 W. Cheyenne Ave., 170-109 Las Vegas, NV 89129 Phone: (702) 825-6060 FAX: (702) 447-8048 matthew.knepper@knepperclark.com miles.clark@knepperclark.com</p> <p>Sean N. Payne Nevada Bar No. 13216 PAYNE LAW FIRM LLC 9550 S. Eastern Ave. Suite 253-A213 Las Vegas, NV 89123 702-952-2733 Fax: 702-462-7227 seanpayne@spaynelaw.com</p>	<p>Thomas A. Zimmerman, Jr. tom@attorneyzim.com Nickolas J. Hagman nick@attorneyzim.com ZIMMERMAN LAW OFFICES, P.C. 77 W. Washington Street, Suite 1220 Chicago, Illinois 60602 (312) 440-0020 telephone (312) 440-4180 facsimile www.attorneyzim.com <i>Pro Hac Vice Application to Be Submitted</i></p> <p>Robert A. Clifford rac@cliffordlaw.com Shannon M. McNulty smm@cliffordlaw.com CLIFFORD LAW OFFICES, P.C. 120 N. LaSalle Street, Suite 3100 Chicago, Illinois 60602 (312) 899-9090 telephone (312) 899-9090 facsimile <i>Pro Hac Vice Application to Be Submitted</i></p> <p>Marc E. Dann Brian D Flick DANNLAW P.O. Box 6031040 Cleveland, OH 44103 Phone: (216) 373-0539 Facsimile: (216) 373-0536 notices@dannlaw.com <i>Pro Hac Vice Application to Be Submitted</i></p>
--	--

Attorneys for Plaintiff and the Class

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA**

RICHARD MCCALL, individually, and on behalf of  
all similarly situated individuals, and HOWARD  
STEPHAN, individually, and on behalf of all  
similarly situated individuals,

Plaintiffs,

v.

EQUIFAX INFORMATION SERVICES, LLC,

Defendant.

Civil Action No.:

**COMPLAINT FOR DAMAGES PURSUANT TO  
THE FAIR CREDIT REPORTING ACT, 15  
U.S.C. § 1681, ET SEQ. AND FOR RELIEF  
UNDER THE DECLARATORY JUDGMENT  
ACT, 15 U.S.C. § 2201, AND FOR DAMAGES  
AND EQUITABLE RELIEF UNDER NEVADA  
LAW  
JURY TRIAL DEMANDED**

### **JURISDICTION AND VENUE**

1. This Court has federal question jurisdiction because this case arises out of violation of federal law, specifically the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681(x) (“FCRA”). 28 U.S.C. §1331; *Smith v. Community Lending, Inc.*, 773 F.Supp.2d 941, 946 (D. Nev. 2011).
2. This Court has supplemental jurisdiction to hear all state law claims under NRS 598C pursuant to 28 U.S.C. § 1367.
3. Venue is proper in the United States District Court for the District of Nevada pursuant to 28 U.S.C. § 1391(b) because Plaintiff is a resident of Clark County, the State of Nevada and because Defendant is subject to personal jurisdiction in the County of Clark, State of Nevada as it conducts business there. Venue is also proper because the conduct giving rise to this action occurred in Nevada. 28 U.S.C. § 1391(b)(2).

### **PARTIES**

4. Plaintiff Richard McCall is a natural person residing in the County of Clark, State of Nevada. Plaintiff and all putative Class members are “consumers” as that term is defined by 15 U.S.C. § 1681a(c).
5. Plaintiff Howard Stephan is a natural person residing in the County of Clark, State of Nevada. Plaintiff and all putative Class members are “consumers” as that term is defined by 15 U.S.C. § 1681a(c).

6. Defendant Equifax Information Services, LLC is a limited liability company incorporated under the laws of the State of Georgia with its principal place of business located at 1550 Peachtree Street NE, Atlanta, GA and doing business in the State of Nevada.
7. Defendant Equifax regularly assembles and/or evaluates consumer credit information for the purpose of furnishing consumer reports to third parties, and uses interstate commerce to prepare and/or furnish the reports. Equifax is a “consumer reporting agency” as that term is defined by 15 U.S.C. § 1681a(f). Equifax is also a “Consumer Reporting Agency that Compiles and Maintains Files on Consumers on a Nationwide Basis” as that term is defined under 15 U.S.C. § 1681a(p).
8. Unless otherwise indicated, the use of Equifax’s name in this Complaint includes all agents, employees, officers, members, directors, heirs, successors, assigns, principals, trustees, sureties, subrogees, representatives, and insurers of Equifax.

### **INTRODUCTION**

9. The United States Congress has found the banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence, which is essential to the continued functioning of the banking system. Congress enacted the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* (“FCRA”), to insure fair and accurate credit reporting, promote efficiency in the banking system, and, as most relevant to this Complaint, protect consumer privacy. The FCRA imposes duties on the CRA's to protect consumer's sensitive personal information.

10. The FCRA protects consumers through a tightly wound set of procedural protections from the material risk of harms that otherwise follow from the compromise of a consumer's sensitive personal information. Thus, through the FCRA, Congress struck a balance between the credit industry's desire to base credit decisions on accurate information, and a consumer's substantive right to protection from damage to reputation, shame, mortification, and emotional distress that naturally follows from the compromise of a person's identity.
11. A central duty that the FCRA imposes upon CRAs is the duty to protect the consumer's privacy by guarding against inappropriate disclosure to third parties. 15 U.S.C. § 1681b codifies this duty, and permits a CRA to disclose a consumer's information only for one of a handful of exclusively defined "permissible purposes." To ensure compliance, CRAs must maintain reasonable procedures to ensure that such third party disclosures are made exclusively for permissible purposes. 15 U.S.C. § 1681e(a).
12. The FCRA defines "consumer report" broadly, as "any written, oral, or other communication of any information by a CRA bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d).

13. The FCRA also entitles the consumer to take an active role in the protection of his or her sensitive personal information, by giving the consumer a right to request “All information in the consumer’s file at the time of the request.” 15 U.S.C. § 1681g(a)(1). Through immediate review of the details of when, and for what purpose, a consumer’s information has been disclosed to a third party, a consumer may better understand whether their identity has been stolen.
14. The FCRA also entitles consumers to actively protect their privacy rights in cases of suspected identity theft. Specifically, a consumer who believes he or she has been the victim of identity theft can submit a fraud alert to a consumer reporting agency. 15 U.S.C. § 1681c-1. The consumer can either request that the fraud alert be imposed for a 90-day period, or for an extended period of seven years. 15 U.S.C. § 1681c-1(a)-(b). In the event a consumer requests “extended” protection, a consumer reporting agency must remove the consumer from any list of third parties to whom the agency sends the consumer’s information to extend firm offers of credit, and keep the consumer off of any such a list for five years, unless the consumer requests otherwise. 15 U.S.C. § 1681c-1(b)(1)(B). After being notified of a fraud alert, a CRA must send notification of the alert to the consumer reporting agencies which report information on a nationwide basis. 15 U.S.C. § 1681c-1(a)(1)(B); *see* 15 U.S.C. § 1681a(p).
15. After fraud notification, the FCRA provides the consumer additional rights to independently monitor their credit information to protect their privacy. Specifically, once notified of a consumer’s fraud notification, a CRA must, within three days of the

notification, provide the consumer with all of the disclosures required under 15 U.S.C. § 1681g. 15 U.S.C. §§ 1681c-1(a)(2), 1681c-1(b)(2). When a consumer requests that an “extended” fraud alert be placed on their files, the consumer is entitled to request two free disclosures under 15 U.S.C. § 1681g within the 12-month period following notification of a fraud alert. 15 U.S.C. § 1681c-1(b).

16. Thus, through immediate review of the details of when, and for what purpose, a consumer’s private information has been disclosed to a third party, a consumer may better understand whether their identity has been stolen. And through semi-annual review of their consumer disclosures in the case of an “extended” alert, a consumer can periodically check to determine whether efforts to protect their identity after potential fraud have not been successful. Thus, the FCRA presupposes that consumers subject to potential fraud should be permitted the immediate opportunity to investigate the issues themselves and ascertain the extent of any suspected fraud.
17. Plaintiffs, individually and on behalf of those similarly situated, bring this action to challenge the actions of Defendant in the protection and safekeeping of the Plaintiffs and Class members’ personal information.
18. Defendant failed to properly safeguard the information of Plaintiffs and Class members, as required under 15 U.S.C. § 1681e(a).
19. Defendant’s violation of 15 U.S.C. § 1681e(a) also “relat[ed] to the sale . . . of goods or services,” and thus violated NRS 598.0923(3). As alleged below, Defendant also violated NRS 598.0917(3) and (7) by engaging in “bait and switch” advertising.

Equifax's violations of NRS and 598.0923(3) and 598.0917(3) and (7) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

### **GENERAL ALLEGATIONS**

20. On or before July 29, 2017, Equifax discovered that one or more of its servers, which contained Plaintiffs' and Class members' sensitive personal information including their names, full Social Security numbers, birth dates, addresses, and, upon belief, their driver's license numbers and possibly one or more of their credit cards ("PII"), had been breached or "hacked" by a still unknown third party ("Data Breach"). According to Equifax, the PII implicated in the Data Breach had "potentially impact[ed] approximately 143 million U.S. consumers."<sup>1</sup>
21. Upon belief, when Equifax discovered this breach, Equifax conducted an internal investigation and contracted with an unidentified third-party cybersecurity firm to conduct a comprehensive forensic review to determine the scope of the hack including identifying the specific data impacted. As of the filing of this Complaint, that investigation remains ongoing and has yet been completed despite over six weeks elapsing since the initial breach.

---

<sup>1</sup> According to Equifax, the breach included personal identifying information including "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers." *Equifax Announces Cybersecurity Incident Involving Consumer Information*, Equifax, Sept. 7, 2017, available at: <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>. Equifax delegates numerous aspects of its consumer-dispute obligations under 15 U.S.C. § 1681i to third-party vendors, including vendors who operate offshore. *See Hiep Le v. Equifax*, No. 16-cv-2393-RFB-GWF, ECF Dkt. 26, at ¶ 4 (D. Nev. Aug. 24, 2017) (internal citations omitted).

22. Between August 1-2, 2017, before the fact of the breach was made public, at least three Equifax executives sold at least \$1.8 million worth of Equifax shares of stock.<sup>2</sup>
23. On September 7, 2017, major news outlets began reporting about the July 29, 2017 incident.<sup>3</sup>
24. For Plaintiffs, as with all potential Class members, these news stories were the first time that they had been informed by Equifax or any credit reporting agency that their information secured by Equifax had been compromised up to six (6) weeks earlier, and they now live in constant fear that their information has been compromised.
25. Equifax's decision to wait six (6) weeks after the alleged data breach before informing all consumers of the same was willful, or at least negligent. Further, by depriving Plaintiffs and Class members information about the breach in a timely manner, Equifax subjected each consumer to a concrete informational injury, as these consumers were deprived of their opportunity to meaningfully consider and address issues related to the potential fraud, as well as to avail themselves of the remedies available under the FCRA to prevent further dissemination of their private information.
26. Equifax has been subject to numerous allegations regarding data breaches in the past.<sup>4</sup> In light of Equifax's continual failure to ensure the integrity of its file storage systems in

---

<sup>2</sup> *Equifax Execs Sold Stock Before Hack Was Disclosed*, Paul R. La Monica, CNN MONEY, Sept. 8, 2017, available at: <http://money.cnn.com/2017/09/08/investing/equifax-stock-insider-sales-hack-data-breach/>.

<sup>3</sup> *See, e.g., Massive Equifax Data Breach Could Impact Half of the U.S. Population*, Alyssa Newcomb, NBCNEWS, Sept. 7, 2017, available at: <https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686>.

<sup>4</sup> *See, e.g., A Brief History of Equifax Security Fails*, Thomas Fox-Brewster, FORBES, Sept. 8, 2017, available at: <https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#63dc4270677c>.



light of known defects to the same and its failure to adequately supervise its 3rd party vendors (several of whom are based off-shore and outside of the U.S.), Equifax willfully, or at least negligently, failed to enact reasonable procedures to ensure that consumer reports would only be provided for a permissible purpose. By failing to establish reasonable procedures to safeguard individual consumer's private information, Equifax deprived millions of consumers from a benefit conferred on them by Congress, which, now lost, cannot be reclaimed.

27. The harm to Plaintiffs and Class members was complete at the time the unauthorized breaches occurred, as the unauthorized disclosure and dissemination of private credit information causes harm in and of itself.
28. Also on September 7, 2017, Equifax began to offer consumers like the Plaintiffs and Class members an allegedly dedicated secure website where consumers could determine if their information was compromised (<https://www.equifaxsecurity2017.com>) and offer consumers "free" credit monitoring through an Equifax product, TrustedID Premier (<https://www.equifaxsecurity2017.com/enroll/>), for one year.
29. However under the guise of an effort to mitigate damages and to provide some assistance to the victims of their data breach, including the Plaintiffs and Class Members, by allowing them free access to their TrustedID Premier service, the terms and conditions of that free service require that the victims, including Plaintiffs and Class members, waive their right to bring or participate in a class action lawsuit and requires them to submit to

arbitration.<sup>5</sup> That is another avenue to deprive the Plaintiffs and Class members of the ability to avail themselves of the remedies available under applicable law to prevent further dissemination of their private information.

30. The Plaintiffs named herein expressly reject the “Terms of Use” (TOU) and have “opted out” by operation of law (since the TOU violated public policy).
31. Moreover, concurred with the filing of the instant complaint, Plaintiffs (on behalf of themselves and those similarly situated) mailed a copy of this Complaint to Equifax Consumer Services LLC, Attn.: Arbitration Opt-Out, P.O. Box 105496, Atlanta, GA 30348.
32. As provided above, this Complaint provides Equifax with notice of Plaintiffs’ and each Class members’ name *and* address. Upon information and belief, Plaintiffs and the Class members were provided an “Equifax User ID”, so this information cannot be provided, since Equifax has simply withheld such information from Plaintiffs and the Class members; or intends that Plaintiffs’ and the Class members’ names and addresses to sufficiently act as an “Equifax User ID” for the stated purpose intended by Equifax; or both.
33. Further, although filing this class action lawsuit should in itself provide Equifax with the “clear statement that [each plaintiff named herein and those similarly situated] do[es] not wish to resolve disputes with Equifax through arbitration”, Plaintiffs and the Class

---

<sup>5</sup> See *Terms of Use*, EQUIFAX, available at: <http://www.equifax.com/terms/>. The “TrustedID Premier” products available from Equifax also contain terms and conditions which suggest that use of the products subjects the using consumer to an arbitration agreement. See *TrustedID Premier Terms of Use*, EQUIFAX, available at: <https://trustedidpremier.com/static/terms>.

members they seeks to represent, hereby definitively state that they do not wish to resolve their disputes with Equifax through arbitration and have opted to bring this class action litigation and rejected (to the extent it has any legal significance – which it does not) the Equifax TOU.

### **CLASS ALLEGATIONS**

34. Plaintiffs bring this action on behalf of a nationwide class of all similarly situated individuals (“Class”), defined as:

All persons in the United States for whom Equifax stored private, personal information that was released as a result of the data breach.

Excluded from the Class are: (1) Defendant, Defendant’s agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities’ current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge’s immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

35. Plaintiffs also bring this action on behalf of a subclass of all similarly situated individuals in Nevada (“Subclass”), defined as:

All persons in Nevada for whom Equifax stored private personal information that was released as a result of the data breach.

Excluded from the Subclass are: (1) Defendant, Defendant’s agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities’ current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge’s immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

36. At this time Plaintiffs do not know the size of the Class because the information is exclusively in the possession of the Defendant, but Plaintiffs believe that the potential number of Class members is so numerous that joinder would be impracticable. It has been reported that the Class could consist of over 100 million people. The number of Class members can be determined through discovery, particularly investigation of Equifax's internal records.
37. All members of the Class have been subject to and affected by a uniform course of conduct in that all Class members' personal information was compromised during the data breach. These are questions of law and fact common to the proposed Class that predominate over any individual questions. The questions common to all Class members include, but are not limited to:
- a. Whether Defendant had implemented reasonable procedures to ensure that all third parties who accessed Plaintiffs' and Class members' private credit information did so for a permissible purpose;
  - b. Whether Defendant failed to notify consumers of the data breach within a reasonable period of time;
  - c. Whether Defendant failed to block the reporting of information on consumers' files that were the result of the data breach;
  - d. Whether Plaintiffs and Class members suffered damages as a result of Defendant's failure to comply with FCRA and NRS 41.600 based on the improper dissemination of their credit information as a result of the data breach;
  - e. Whether Plaintiffs and Class members are entitled to statutory damages; and
  - f. Whether Plaintiffs and Class members are entitled to punitive damages.

38. Plaintiffs' claims are typical of the Class, as Plaintiffs' personal information was compromised during the data breach. All claims are based on the same legal and factual issues.
39. Plaintiffs will adequately represent the interests of the class and do not have an adverse interest to the Class. If individual Class members prosecuted separate actions, it may create a risk of inconsistent or varying judgments that would establish incompatible standards of conduct. A class action is the superior method for the quick and efficient adjudication of this controversy. Plaintiffs' counsel have experience litigating consumer class actions.
40. Further, under Fed. R. Civ. Pro. 23(a), Defendant acted on grounds generally applicable to the proposed Class, making appropriate final declaratory and injunctive relief with respect to the proposed Class as a whole.

**COUNT ONE: VIOLATION OF 15 U.S.C. §1681, et al.**

41. Plaintiffs restate all allegations contained in Paragraphs 1 through 40 as if fully rewritten herein.
42. This Count is brought on behalf of the nationwide Class.
43. Based upon Equifax's failure to have reasonable procedures in place, Plaintiffs' and Class members' private information was compromised, and neither Plaintiffs nor Class members received notice of the data breach, except through the media, approximately six (6) weeks after the breach occurred.

44. As a result of each and every willful violation of FCRA, Plaintiffs and Class members are entitled to: actual damages, pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages, pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages, as this Court may allow, pursuant to 15 U.S.C. 1681n(a)(2); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681n(a)(3).
45. As a result of each and every negligent non-compliance of the FCRA, Plaintiffs and Class members are also entitled to actual damages, pursuant to 15 U.S.C. § 1681o(a)(1); and reasonable attorney's fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from Defendant.

**COUNT TWO: VIOLATION OF NRS 41.600**

46. Plaintiff repeat and re-allege Paragraphs 1 through s45, with the same force and effect as though fully set forth herein.
47. This Count is brought on behalf of the Nevada Subclass.
48. Defendant's violation of 15 U.S.C. §1681e(a) also "relat[ed] to the sale . . . of goods or services," and thus violated NRS 598.0923(3). Equifax's violations of NRS 598.0915(15) and 598.0923(2) and (3) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).
49. Defendant engaged in unfair and unlawful acts and practices by failing to maintain adequate procedures to avoid a data breach, furnishing consumer reports that Defendant has reasonable grounds to believe will not be used for a proper purpose, and failing to notify Plaintiffs and Subclass members of the data breach within a reasonable time.

50. Defendant engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiffs and Subclass members.
51. As a direct and proximate result of the foregoing, Plaintiffs and Subclass members have suffered injuries including, but not limited to mental anguish, emotional distress, fear, panic, stress, and the continued worry that their identities have been compromised and are being used fraudulently.
52. Through its offer of a “free” service of credit monitoring, Defendant engaged in a “bait and switch” which is prohibited under the NRS 598.0917 by trying to trick Nevada consumers into signing a broad class action waiver and arbitration agreement, which would benefit only Equifax.
53. This “bait and switch” advertising violated NRS 598.0917(3) because it constituted “an offer to sell . . . services which the seller . . . in truth may not intend or desire to sell or lease,” which was accompanied by a requirement of other undisclosed conditions before selling the goods. The advertising was also violated NRS 598.0917(7) because it constituted a tender of “goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised.”

### **COUNT THREE: DECLARATORY JUDGMENT**

54. Plaintiffs repeat and re-allege Paragraphs 1 through 53, with the same force and effect as though fully set forth herein.
55. At all relevant times, there was in effect the Declaratory Judgment Act (“DJA”), 8 U.S.C. § 2201(a), which states, in relevant part:

In a case of actual controversy within its jurisdiction . . . any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such.

28 U.S.C. § 2201(a).

56. Plaintiffs and Class members seek an order declaring that the arbitration clause and class action waiver in the Equifax and TrustedID Premier Terms of Use are invalid and do not apply to any claims they may have arising out of the data breach.
57. The controversy presented in this case is definite and concrete, and affects the adverse legal interests of the parties. As a result of the data breach and the release of Plaintiffs' and Class members' private personal information, Plaintiffs and Class members are at a great risk of having that personal information used by unauthorized individuals.
58. To safeguard against the unauthorized use of the personal information that was kept by Defendant, Plaintiffs and Class members must obtain credit monitoring. The need for credit monitoring is urgent, as the information that Equifax failed to safeguard is extremely sensitive and can be used to steal Plaintiffs' and Class members' identities, which can lower their credit scores, cost money, and cause severe emotional distress.<sup>6</sup>

---

<sup>6</sup> (See *Victims of Identity Theft, 2014*, Erika Harrell, Ph.D., U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, (Sept. 2015), available at: <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (stating that half of the victims of identity theft suffered losses of more than \$100, identity theft losses totaled more than \$15.4 billion in 2014, and identity theft victims frequently experience "moderate or severe emotional distress as a result of the incident."))



59. Defendant established a website that allows individuals to check to see if their personal information is at risk, and it allows individuals to enroll in a year of free credit monitoring through Defendant's credit monitoring program, TrustedID Premier.
60. However, the "TrustedID Premier Terms of Use" include provisions that require enrollees to settle all disputes with Defendant—including Defendant's failure to adequately safeguard Plaintiffs' and Class members' private personal information—through binding, individual arbitration, "even if the facts and circumstances upon which the claims are based already occurred or existed."<sup>7</sup> The Equifax terms of use contain similarly limiting language regarding use of its website.<sup>8</sup>
61. As such, Defendant is requiring all Class members to waive their right to participate in a class action for their claims arising out of the data breach, and to submit their individual claims to arbitration, before Defendant will assist those individuals with necessary credit monitoring to prevent the harm that Defendant has caused.
62. The only other option Class members have to protect themselves is to pay for credit monitoring on their own. For Class members who cannot afford to purchase credit monitoring on their own, they are forced to either waive their right to participate in a class action, or forego any credit monitoring and face the risk of identity theft without any protection.
63. Further, many individuals have reported that even when inputting fake or incorrect information into Defendant's website, Defendant still informs those individuals that their

---

<sup>7</sup> See *TrustedID Premier Terms of Use*, EQUIFAX, available at: <https://trustedidpremier.com/static/terms>

<sup>8</sup> See *Terms of Use*, EQUIFAX, available at: <http://www.equifax.com/terms/>.

- personal information is part of the data breach, and that they should sign up for Defendant's credit monitoring, thereby waiving any right to participate in a class action.<sup>9</sup>
64. Moreover, if the individual does not cancel Defendant's credit monitoring program by calling Defendant, Defendant will begin charging those individuals for the credit monitoring after one year.<sup>10</sup> As a result, Defendant will profit off of those persons who were harmed by Defendant's failure to adequately safeguard Plaintiffs' and Class members' personal information.
65. Therefore, enforcing the arbitration clause and class action waiver in the Equifax and TrustedID Premier Terms of Use is unfair to Plaintiffs and Class members, because the waivers are obtained through duress, harm Plaintiffs and Class members, and are unconscionable.
66. There is an actual controversy between the parties of sufficient immediacy and reality to warrant the issuance of a declaratory judgment because Defendant is requiring Class members to (a) waive legal rights they have against Defendant in order to prevent additional harm with Defendant's credit monitoring, (b) pay for credit monitoring themselves, or (c) forego credit monitoring altogether.
67. Consequently, Plaintiffs and Class members have been, and will continue to be, caused significant harm in that they must choose between waiving legal rights or risking additional identity theft. Plaintiffs and Class members will continue to suffer harm if the

---

<sup>9</sup> See *Why Some Are Recommending "Credit Freezes" in the Wake of the Gigantic Equifax Data Breach*, Tom McKay, Gizmodo, Sept. 9, 2017, available at: <http://gizmodo.com/why-some-are-recommending-credit-freezes-in-the-wake-1802924951>

<sup>10</sup> See *id.*

Court were to deny their request for declaratory relief, as the harm of identity theft is ongoing.

68. If the Court were to deny Plaintiffs' and Class members' request for declaratory relief, this controversy will continue to exist, as they must continue to pay for credit monitoring or risk additional identity theft, or waive legal rights against Defendant, and many Class members will continue to face this dilemma until this case is resolved.
69. There are no disputed legal and factual issues that the Court would have to resolve in granting Plaintiffs' and Class members' request for declaratory relief, as this issue does not affect the merits of Plaintiffs' and Class members' claims against Defendant, and instead seeks to preserve the *status quo*—i.e., that Plaintiffs and Class members have the right to pursue their claims against Defendant arising out of the data breach in Court as part of a class action lawsuit.
70. Based on the foregoing facts, the Court should declare the arbitration clause and class action waiver in the Equifax and TrustedID Premier Terms of Use are invalid and do not apply to any claims they may have arising out of the data breach.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request the following relief against Defendant Equifax Information Services, LLC:

- A. For an award of actual damages against Defendant for all allegations contained in Count One and Count Two;
- B. For an award of statutory damages pursuant to 15 U.S.C. §1681n(a)(1) against Defendant for the allegations contained in Count One for each eligible Class member and the Plaintiffs;

- C. For an award of punitive damages against Defendant for the allegations contained in Count One and Count Two as this Court may allow pursuant to 15 U.S.C. §1681n(a)(2);
- D. For an award of the costs of litigation and reasonable attorneys' fees pursuant to 15 U.S.C. §1681n(a)(3) and 15 U.S.C. §1681(o)(1)(1) against Defendant for each incident of noncompliance of FCRA alleged in Count One and under NRS 41.600(c) as alleged in Count Two;
- E. For an order declaring the arbitration clause and class action waiver in the TrustedID Premier Terms of Use are invalid and do not apply to any claims Plaintiffs and the Class members may have arising out of the data breach;
- F. For a preliminary and permanent injunction prohibiting Equifax from continuing to bait and switch consumers into signing a class action waiver and arbitration agreement that would apply to any claims they may have arising out of the data breach; and

...

...

...

...

G. For all other relief this Court may deem just and proper.

**JURY DEMAND**

Plaintiffs hereby request a trial by jury on all issues so triable.

Dated: September 10, 2017

Respectfully Submitted,

<p><u>/s/ David H. Krieger</u> David H. Krieger, Esq. George Haines, Esq. HAINES &amp; KRIEGER, LLC 8985 S. Eastern Ave., Suite 350 Henderson, NV 89123</p> <p>Matthew I. Knepper, Esq. Miles N. Clark, Esq. KNEPPER &amp; CLARK LLC 10040 W. Cheyenne Ave., 170-109 Las Vegas, NV 89129</p> <p>Sean N. Payne PAYNE LAW FIRM LLC 9550 S. Eastern Ave. Suite 253-A213 Las Vegas, NV 89123</p>	<p>Thomas A. Zimmerman, Jr. Nickolas J. Hagman ZIMMERMAN LAW OFFICES, P.C. 77 W. Washington Street, Suite 1220 Chicago, Illinois 60602 <i>Pro Hac Vice Application to Be Submitted</i></p> <p>Robert A. Clifford Shannon M. McNulty CLIFFORD LAW OFFICES, P.C. 120 N. LaSalle Street, Suite 3100 Chicago, Illinois 60602 <i>Pro Hac Vice Application to Be Submitted</i></p> <p>Marc E. Dann Brian D Flick DANNLAW P.O. Box 6031040 Cleveland, OH 44103 <i>Pro Hac Vice Application to Be Submitted</i></p>
--	---

*Counsel for the Plaintiff and the Class*